# Red-Teaming the NCAE Cyber Games

Spencer Hall- NCAE Cyber Games Red Team Co-lead
James Rice- NCAE Cyber Games Participant Preparation Lead

NCAE CYBER GAMES
PLAY | LEARN | PROTECT

# Where we started (First joined the team)

ftp.sh 408 B

```
#!/bin/bash
IP="$1"
FILE=TPS_Report.txt
USER=peter
PASS=[redacted]

wget --timeout=3 --tries=1 --user=$USER --password=$PASS ftp://$IP/$FILE
rc=$?

# If file was recieved, then check is good
if [ "$FILE" ]; then
    rm "$FILE"
    exit 0
fi

# Couldn't connect to FTP
if [ $rc -eq 1 ]; then
    exit 2
fi

# We connected to FTP but file not found
exit 1
```

setup_grub_timer.sh 529 B

```
#!/bin/bash
#
# File: setup_grub_timer.sh
# Sets the grub timer to parameter passed and ensures the grub timer is
# not hidden. Default timer is 15
#
# Parameters:
# 1 - time in seconds
# 2 - file path to the grub config

set -e

if [[ ${EUID} -ne 0 ]]; then
    echo "Run as root!"
    exit 1
fi

timer="${1:-15}"
fpath="${2:-/etc/default/grub}"

# Replace the entire GRUB_TIMEOUT line
sed -i "/GRUB_TIMEOUT=/c\GRUB_TIMEOUT=${timer}" "${fpath}"
sed -i "/^GRUB_TIMEOUT_STYLE=/c\#GRUB_TIMEOUT_STYLE=hidden" "${fpath}"
update-grub
```

```
function configureMySQL {
    if ! apt list --installed | grep -q mysql-server; then
        echo "MySQL not installed!"
        exit 1
    fi
    if [[ ! -f ${CONF} ]]; then
        echo "Could not find the file ${CONF}"
        exit 1
    fi

    # mysqld directive doesnt exist, add it and config line
    if ! grep -q "\[mysqld\]" "${CONF}"; then
        echo "[mysqld]" >> "${CONF}"
        echo "skip-grant-tables" >> "${CONF}"
    else
        # add our config line after mysqld directive
        sed -i 's/\[mysqld\]/\[mysqld\]\nskip-grant-tables/g' "${CONF}"
    fi
}

configureMySQL
```

# Where we initially expanded

```
$ docker-compose exec -it provisioner pvs
loaded 0 YAML plugin(s) from /data/provisioner/provisioner/plugins
loaded 1 Python plugin(s) from /data/provisioner/provisioner/plugins
loaded 73 YAML plugin(s) from ../provisioner-plugins
loaded 0 Python plugin(s) from ../provisioner-plugins
[01:26:36] [default_event] provisioner )> show options
Config                    Value
==========================================================================
job!targets               set()
job!event_id              default_event

ansible!password          None
ansible!user              ansible
ansible!become            True
ansible!become_user       root
ansible!become_password   None
ansible!become_method     sudo
ansible!gather_facts      True
ansible!ssh_key           ~/.ssh/ansible_key
ansible!verbosity         None
ansible!hosts             ['all']

[01:26:40] [default_event] provisioner )>
```

provisioner

```
[01:26:40] [default_event] provisioner )> use grub_timeout
plugin now in use at: plugins.grub_timeout:0
[01:27:09] [default_event] provisioner )> show options
Config                                    Value
==========================================================================
job!targets                               set()
job!event_id                              default_event

ansible!password                          None
ansible!user                              ansible
ansible!become                            True
ansible!become_user                       root
ansible!become_password                   None
ansible!become_method                     sudo
ansible!gather_facts                      True
ansible!ssh_key                           ~/.ssh/ansible_key
ansible!verbosity                         None
ansible!hosts                             ['all']

plugins.grub_timeout:0!grub_timeout       30
plugins.grub_timeout:0!grub_path          /etc/default/grub
plugins.grub_timeout:0!altitude           10000

[01:27:11] [default_event] provisioner )>
```



CAE IN CYBERSECURITY COMMUNITY

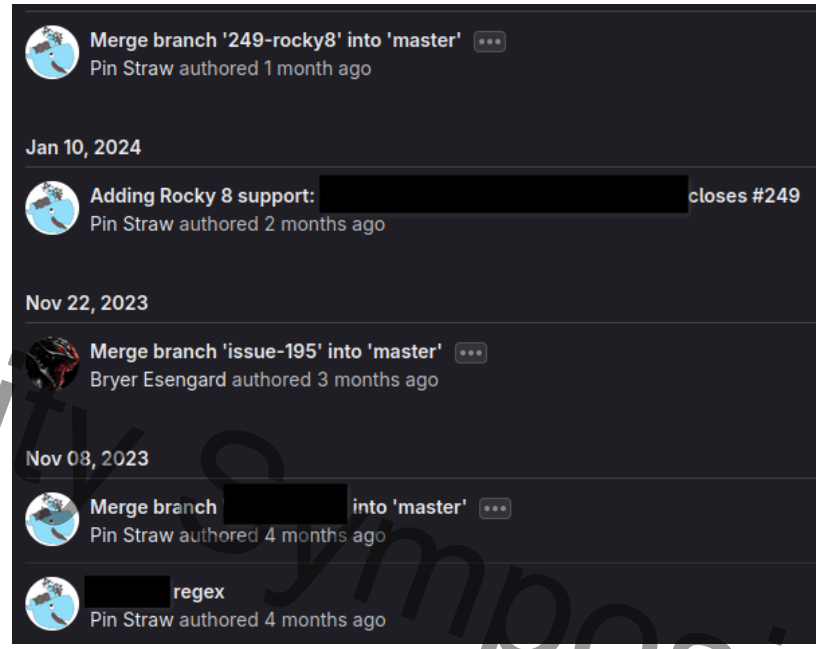
NCAE CYBERGAMES

PLAY | LEARN | PROTECT

# Building out

bind_setup/tasks/main.yml 0 → 100644

```
+ ---
+ - name: Including OS Specific Variables
+   include_vars:
+     file: "{{ ansible_os_family }}.yml"
+
+ - name: Include Bind Template Variables
+   include_vars:
+     file: "Bind.yml"
+
+ - name: Install Bind Packages
+   package:
+     name: "{{ bind_packages }}"
+     state: present
+   loop: "{{ __bind_packages }}"
+   loop_control:
+     loop_var: bind_packages
+
+ - name: Ensure Zone Directory is Created
+   file:
+     path: "{{ zone_dir }}"
+     state: directory
+     owner: root
+     group: root
+     mode: "0755"
+
+ - name: Create Bind Conf File
+   template:
+     src: templates/named.conf
+     dest: "{{ bind_conf }}"
+     owner: root
+     group: "{{ bind_group }}"
+     mode: "0666"
```



# VM Automation

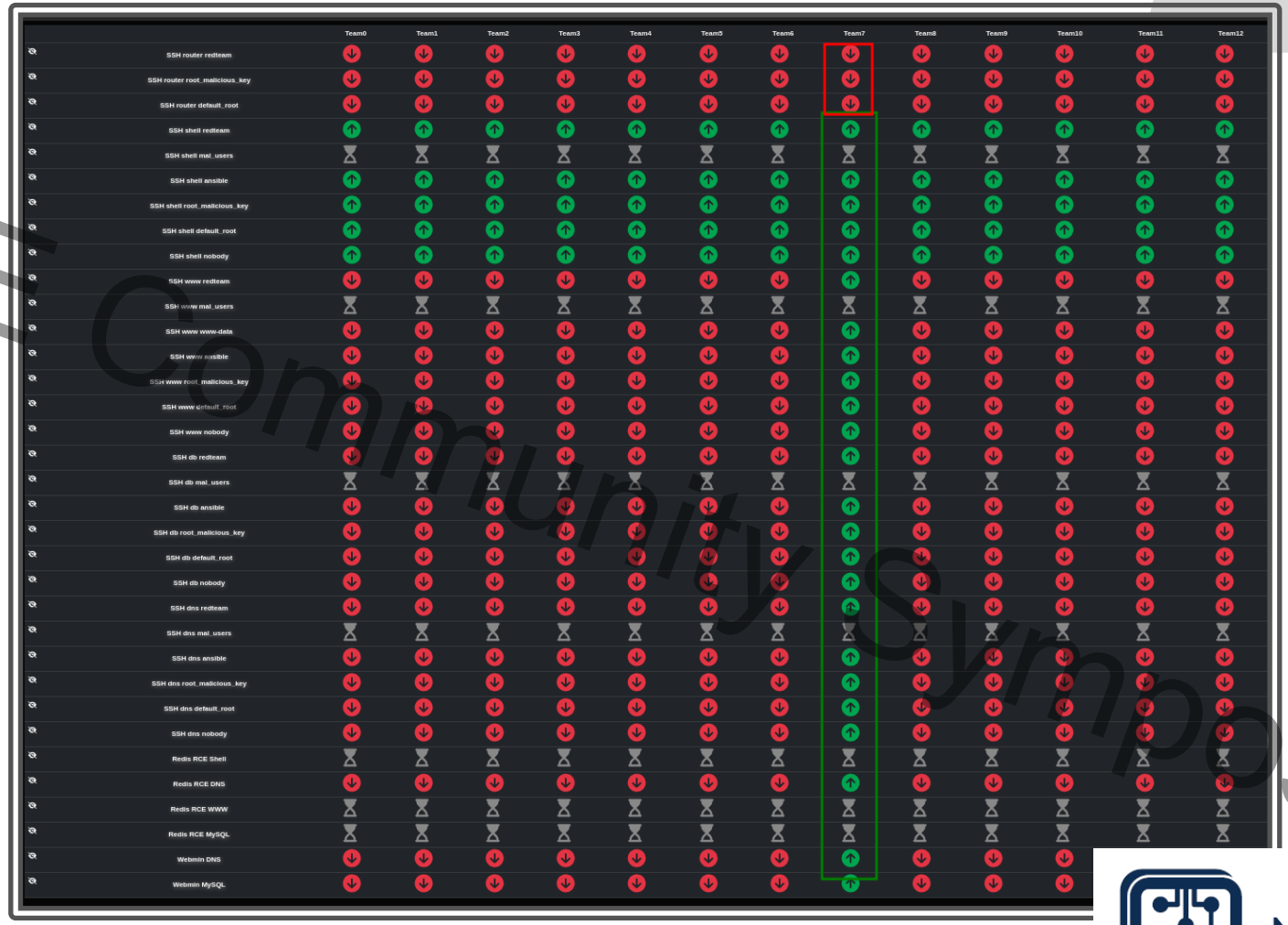


initial rocky9 template
Pin Straw authored 1 month ago
62da1fe8

| Name | Last commit | Last update |
|---|---|---|
| kali-template | Creating redteam kali template | 2 months ago |
| rocky9 | initial rocky9 template | 1 month ago |
| .gitignore | Creating redteam kali template | 2 months ago |
| LICENSE | Adding LICENSE file | 4 months ago |
| README.md | Initial commit | 4 months ago |

```
PLAY RECAP *********************************************************************
172.18.255.112             : ok=211  changed=80   unreachable=0    failed=0    skipped=7    rescued=0    ignored=1
172.18.255.143             : ok=211  changed=80   unreachable=0    failed=0    skipped=7    rescued=0    ignored=1
172.18.255.163             : ok=208  changed=75   unreachable=0    failed=0    skipped=10   rescued=0    ignored=0
172.18.255.170             : ok=211  changed=80   unreachable=0    failed=0    skipped=7    rescued=0    ignored=1
172.18.255.195             : ok=208  changed=75   unreachable=0    failed=0    skipped=10   rescued=0    ignored=0
172.18.255.57              : ok=208  changed=75   unreachable=0    failed=0    skipped=10   rescued=0    ignored=0
172.18.255.60              : ok=208  changed=75   unreachable=0    failed=0    skipped=10   rescued=0    ignored=0
172.18.255.72              : ok=208  changed=75   unreachable=0    failed=0    skipped=10   rescued=0    ignored=0

Status changed to: successful
Ansible task is complete
Runner successful
[04:22:05] [default_event] provisioner )>
```

# Further Insight






CAE IN CYBERSECURITY COMMUNITY

NCAE CYBERGAMES
PLAY | LEARN | PROTECT

# Importance?

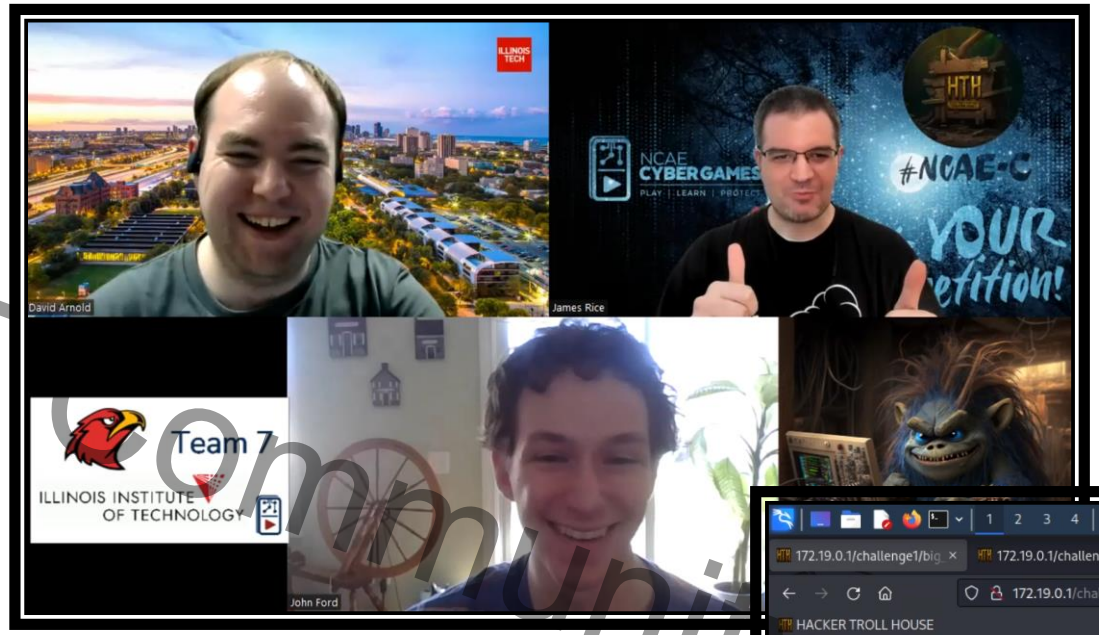
```
Training: >
  Students should be aware of the software and the modules that it has loaded. Modules that
  provide unnecessary or possibly malicious capabilities should be removed.

Justification: >
  This challenge covers the skills required to analyze and evaluate
  the system's environment and identify suspicious additions to their system's configuration.
  The student must demonstrate that they determine a malicious module in legitimate software,
  and reconfigure the software to a functional and secure state.
```

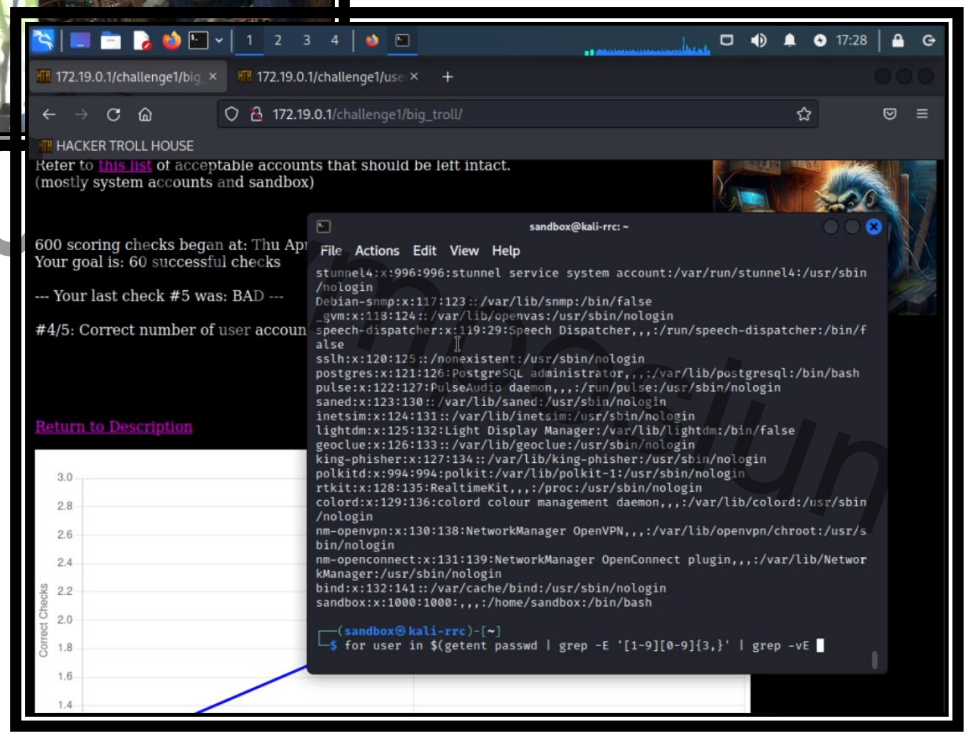
```
Training: >
  Students should be aware of how the package managers work on their system
  and where to look at the common configurations of them. By familiarizing themselves
  with different packages managers they will be able to move efficiently debug
  issues when trying to install packages.

Justification: >
  This challenge covers the skills required to properly understand how the
  packages manager works across different Linux distributions and how to
  rectify any issues they may run into when trying to install software.
```

# Hacker Troll House

# 2023-2024 NCAE Cyber Games






Format: 2 students from each team selected for our in-person Invitational event.

Complete a series of fun challenges in a cyber gameshow style experience.


# Questions?



NCAE CYBER GAMES
PLAY | LEARN | PROTECT